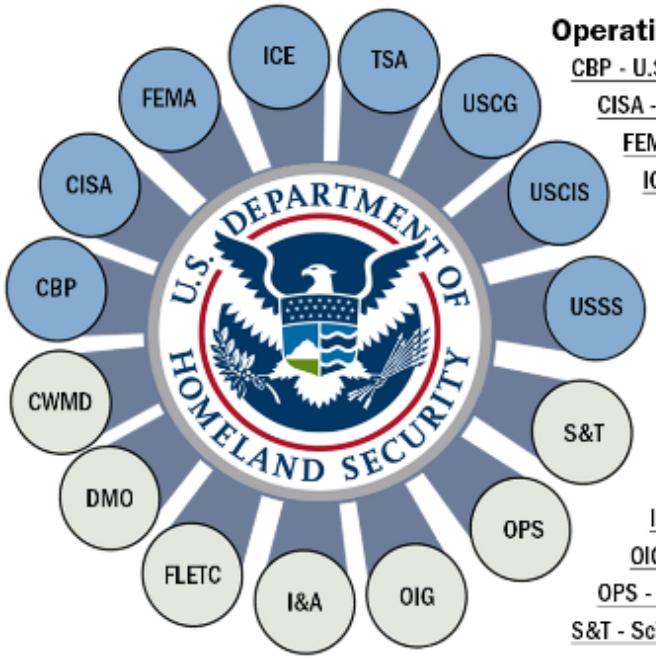
Improving Data Utilization to Increase Operational Effectiveness at DHS

October 30, 2019

Dr. Brian Teeple

Department of Homeland Security
Chief Technology Officer (CTO) and Chief Data Officer (CDO)

Department of Homeland Security (DHS)



Operational Components

CBP - U.S. Customs and Border Protection
CISA - Cybersecurity and Infrastructure Security Agency
FEMA - Federal Emergency Management Agency
ICE - U.S. Immigration and Customs Enforcement
TSA - Transportation Security Administration
USCG - U.S. Coast Guard
USCIS - U.S. Citizenship and Immigration Services
USSS - U.S. Secret Service

Support Components

CWMD - Countering Weapons of Mass Destruction Office*
DMO - Departmental Management and Operations
FLETC - Federal Law Enforcement Training Centers
I&A - Office of Intelligence and Analysis
OIG - Office of Inspector General
OPS - Office of Operations Coordination
S&T - Science and Technology Directorate

Every mission across DHS relies on information sharing.

Turning Data Into Information

Secure the Data (Zero-Trust)

Manage the Data (Data Governance)

Process and Analyze the Data (Data Analytics and Artificial Intelligence)

The value of data is in the ability to inform decision making.

Considerations for Sharing Data

- Proprietary
- Acquisition Sensitive
- Sensitive but Unclassified
- Privacy
- Law Enforcement
- Classified

Verified Trusted Access Anywhere, Anytime, to Any Resource

Zero Trust is a set of security architecture principles that treat all requests for resources as untrusted and requires verified policy alignment at each stage.

Zero Trust security architecture enables:

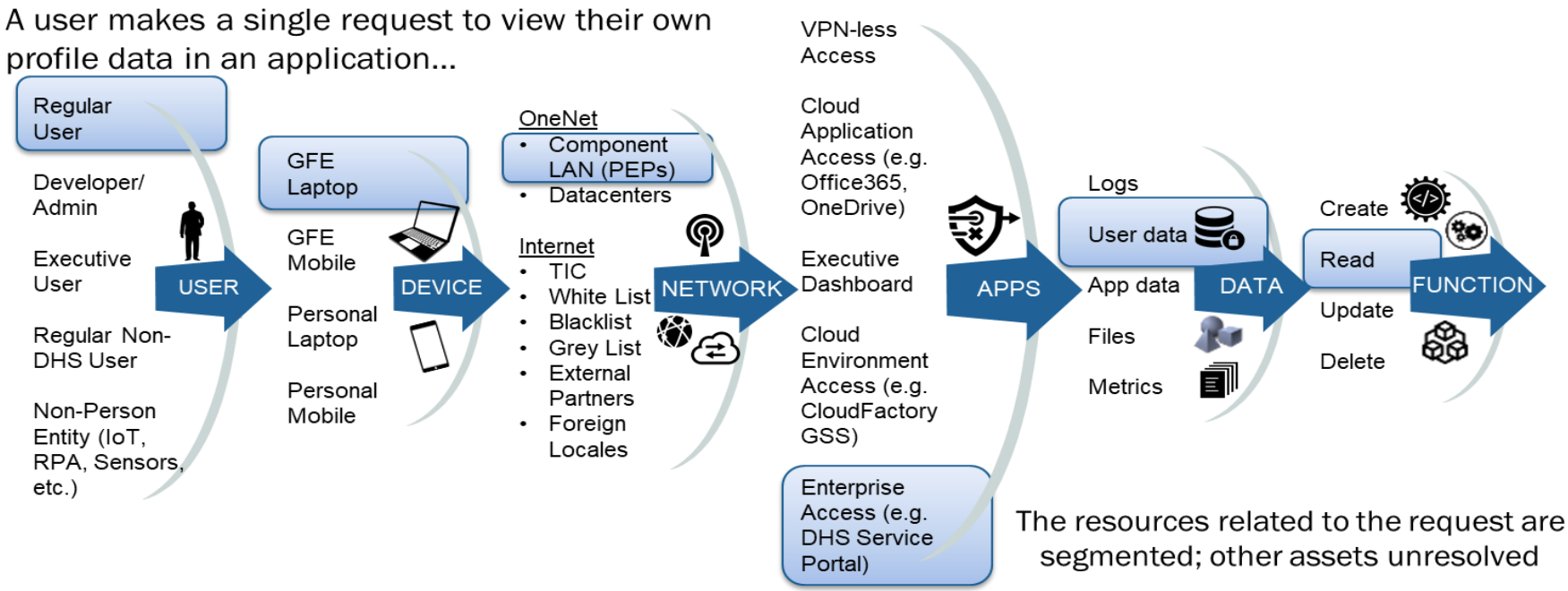
- Managed security for an ever expanding DHS network perimeter
- Unified cloud, mobile, and legacy environments under a single security architecture
- As perimeter expands we need adaptive security to segment requests from unrelated applications
- Improved insight into DHS security posture and improved response to targeted attacks and zero day events.

"Security strategies must be built around a zero trust approach—in other words, one that trusts nothing outside or inside an organization."

Zero Trust: The Modern Approach To Cybersecurity *(Forbes: June 12, 2019)*

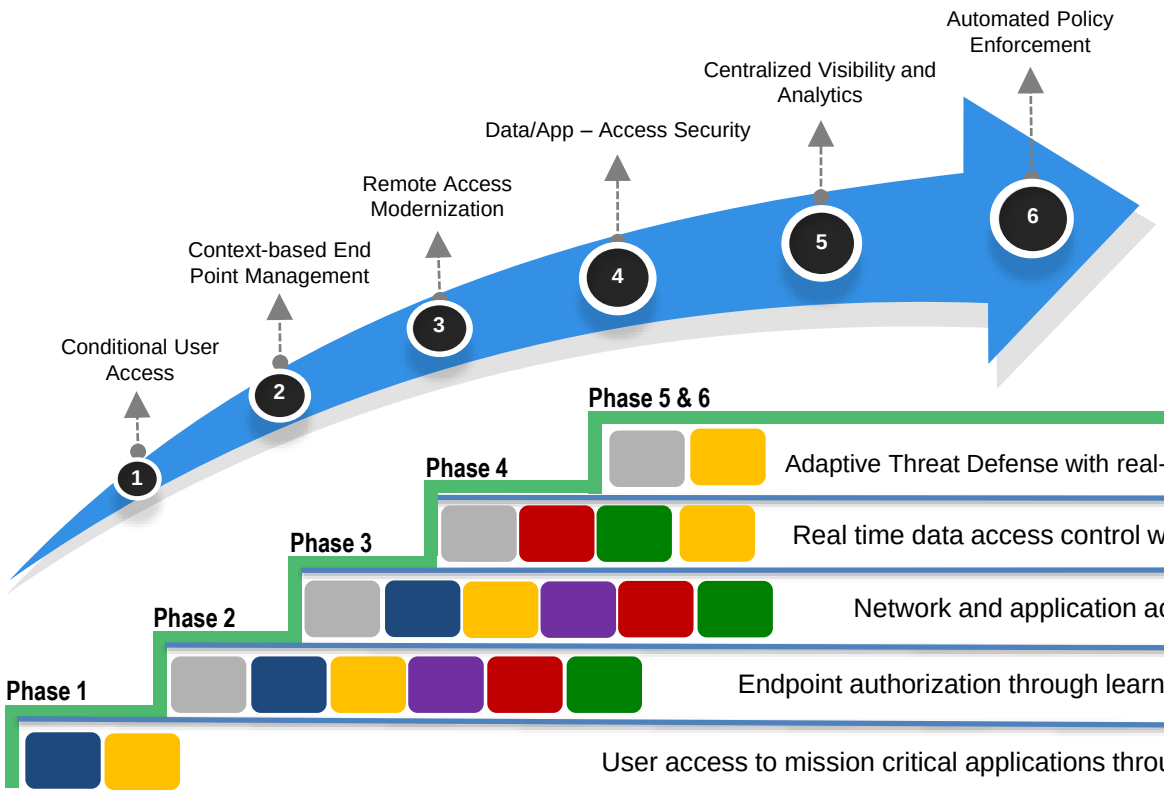
What is DHS Zero Trust? Never Trust – Always Verify

A security architecture that evaluates everything and everyone against a set of conditional security policies with each request before allowing access to only a single resource.



Notional ZT Approach

Incremental approach provides immediate results while building towards final solution



Staged Approach

- Phases comprise multiple 90-120 day security sprints that deliver capability
- Building blocks with capability at each step
- Addresses current security gaps first

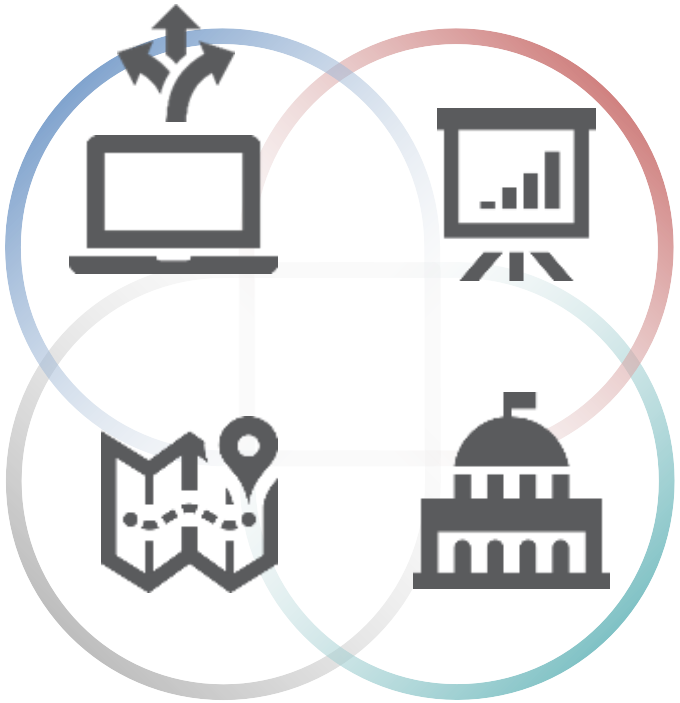
Data Governance - Impetus for Change

Mission Drivers:

- Information Sharing is a core function at DHS
- 2019 DHS Winter Study

Executive Drivers:

- Federal Data Strategy
- Foundations for Evidence Based Policymaking Act of 2018
  - Open Government Data Act of 2019



Constraints with Today's Data Governance and Data Management at DHS

Broad Mission Areas within DHS

- Lack of common data formats
- Lack of standardization and interoperability of data assets
- Lack of accurate data inventories

Data Management Takes Place at Component Levels

- A few Components have established formal CDOs
- Lack of formally established enterprise data governance model
- Addressing tactical problems and internal Component data governance processes

Department level governance and management is loosely matrixed

DHS Enterprise Data Strategic Overview

DHS Enterprise Data Vision

An enterprise where every DHS mission operator and organizational component has timely and reliable access to accurate information needed to accomplish their mission and management activities thought the effective, innovative, and lawful use of DHS and external data.

DHS Enterprise Data Mission

Fully leverage the Department's data assets to enhance mission operations, strategic planning, resource management, and analytics.

DHS Enterprise Data Guiding Principles

Mission Value

Data and the information derived form data are valued departmental assets

Stewardship

DHS will ensure that the processes by which data are collected, produced, governed and managed are open and clear to all stakeholders

Accountability

All data assets in DHS must be inventoried, catalogued, and tracked with a clear demarcation between metadata and content.

Authority and Trust

DHS will identify authoritative DHS standards, including technical and convention standard types, for each form of data.

The Way Forward – 12 Month Crawl

- ✓ Appoint DHS Chief Data Officer and Deputy Chief Data Officer
- ✓ Constitute a DHS Data Governance Body
- DHS OCDO teams with component CDOs and data SMEs to execute the federal data strategy at DHS
- Build out the Advanced Data Analytics Technology Roadmap
- Establish a baseline measure of DHS data maturity and identify data skills and resource needs
- Identify data needs to address the mission
- Initiate plans to secure resources
- Identify priority datasets for Agency Open Data plans
- Keep Going!

Process and Analyze Data

- Structured vs Unstructured Data
- Advances in process automation, data analysis, machine learning and artificial intelligence
  - Assume large quantities of data are available
  - Rely heavily on data quality
  - Tend to be heavily tailored to the question being asked

How do we prioritize?

- Mission needs – what are the most important questions to answer?
- Use the Questions to Drive the Data Needs
  - To Share (Data security)
  - To Manage (Data governance)
  - To Analyze (Data Analytics / AI)

Incremental Approach driven by Mission Needs